ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-23

Hershey Canada Inc.

October 7, 2013

(Case File #P2267)

I. Introduction

[1] Under s. 34.1 of the *Personal Information Protection Act* (PIPA), an organization having personal information under its control must, without unreasonable delay, notify me of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

[2] On February 14, 2013, The Hershey Company (Organization) provided notice of an incident involving the unauthorized access to personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to individuals as a result of the incident. I require that the Organization notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[3] Section 37.1 of PIPA authorizes me to require an organization to notify individuals to whom there is a real risk of significant harm as a result of an incident. It states:

> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
>
> (a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

(2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

(4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), and

(c) to satisfy terms and conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

[4] PIPA applies to organizations, defined in section 1(1)(i) of PIPA as follows:

1(1) (i) "organization" includes

(i) a corporation,

(ii) an unincorporated association,

(iii) a trade union as defined in the *Labour Relations Code*,

(iv) a partnership as defined in the *Partnership Act*, and

(v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

[5] The Organization is federally incorporated. The incident involved the Organization's youth track and field event manager website. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA and it collected personal information from Alberta residents on the website.

[6] The incident involved the following information found in databases associated with the website:

a) adult parents or volunteers:
- name,
- mailing address,
- email address, and
- telephone number.

b) event coordinators:
- name,
- mailing address,
- email address,
- telephone number,
- user name,
- password, and
- answers to security questions for website access.

c) youth track and field participants, ages 9-14 years:
- name,
- age,
- date of birth,
- city,
- province or territory,
- track and field placement in events, and
- with respect to 179 youths who could be linked to adult parents in (a), mailing address and telephone number.

[7] The above information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On March 7, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization March 15, 2013, and May 16, 2013.

[9] The circumstances of the incident as reported to me by the Organization are as follows:

- The youth track and field event manager website is used to coordinate Organization sponsored events across Canada and the United States.
- The Organization website is hosted on a third party server.
- An unauthorized individual(s) accessed the third party server and deployed a malicious script.
- As a result of the malicious script, a website stored on the same server as the Organization website was defaced with a political statement on January 17, 2013.
- When the third party service provider restored the defaced website, the malicious script replaced all default web pages hosted on the server, including the Organization website, with the political statement.
- As a result, the Organization website was defaced with the political statement on January 19, 2013.
- Personal information in the databases associated with the Organization website may have been exposed as a result of this incident.
- The Organization is unable to determine if the databases were accessed as it has no audit capability.
- There were 39 adult parents or volunteers, 66 event coordinators, and 1,820 youths from Alberta, out of a total of 13, 240 Canadians, affected by the incident.
- The website was taken down on January 19, 2013. The Organization retained a new service provider to host the website and imposed stricter security controls.
- The Organization took the following steps to notify affected individuals about the incident:
    - A notification letter or email was sent to adults and event coordinators on February 8, 2013.
    - Conference calls occurred on February 7, 2013, with partners of the track and field events. Information about the incident, the notification letter and a "Frequently Asked Questions" document were provided.
    - A notice and a link to the notification letter were posted on the Organization's track and field websites.
    - An email was sent to event coordinators on May 1, 2013, requesting they contact any youths they had contact with from past or recent events to direct them to the notification on the Organization website.

IV. Is there a real risk of significant harm to individuals as a result of the incident?

[10] In considering whether to require the Organization to notify the affected individuals, I am mindful of PIPA's purpose, legislative principles, and the relevant circumstances surrounding the reported incident.

[11] Pursuant to section 37.1 of PIPA, I have the power to require the Organization to "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure." In determining whether or not to require the Organization to notify the affected individuals, I must consider if there is a "real risk of significant harm" to the affected individuals as a result of the incident.

[12] In order for me to require that the Organization notify the affected individuals, there must be some harm – some damage or detriment or injury – that could be caused to those affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[13] The Organization submitted the incident did not pose a risk of significant harm to the affected individuals. The database did not contain credit card or financial information. With the exception of dates of birth, the youth data was available on the Organization's website.

[14] The personal information of the adults and event coordinators is of low to moderate sensitivity. It includes names, addresses, telephone number, email addresses, passwords for the website, and answers to security questions. The type of harm that could result from unauthorized access to names, addresses, telephone numbers and email addresses is phishing. The type of harm that could result from unauthorized access to name and the answers to security questions is identity theft and fraud (see P2012-ND-30). In my view, these are significant harms.

[15] With respect to the youths, information pertaining to city of residence, province or territory, age and track and field placement are of low sensitivity. However, the names in conjunction with dates of birth of the youths are of moderate sensitivity. An individual's date of birth is widely used as a unique identifier. A date of birth cannot be changed. It remains constant throughout an individual's lifetime. Name and date of birth are recognized in the Criminal Code as "identifying information" which if acquired and used for a criminal purpose, such as identity theft, constitutes a criminal offence. Courts in the United States of America have recognized that the disclosure of dates of birth create a substantial and demonstrable risk to the personal security of individuals in the form of identity theft[1]. The type of harm that could occur to the youths as a result of this incident is identity theft and fraud. In my view, these are significant harms.

[1] *Governor's Office of Administration v. Dylan Purcell*, Commonwealth Court of Pennsylvania, No. 2452 C.C. 2010.

[16] In order for me to require the Organization to notify the affected individuals there must also be a "real risk" of significant harm to these individuals as a result of the incident. This standard does not require that significant harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.

[17] The Organization assessed the real risk of significant harm to the affected individuals as low for the following reasons:

- The personal information was not sensitive.
- There is no information to confirm or deny the databases were actually accessed.
- Websites of other organizations on the compromised server had more valuable information.
- The Organization did not appear to be the original target of the intrusion. The intrusion involved defacement of the website for political purposes unrelated to the Organization.
- With respect to the youths, only the date of birth was not previously published on the website.
- There is not enough information available to enable the Organization to directly contact and notify the majority of the youths, let alone to enable someone to commit identity theft with the personal information involved.

[18] Based on the above and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident. I recognize the Organization website was defaced only after an unrelated website stored on the same server was defaced and repaired by the service provider. I agree with the Organization that it does not appear the intrusion was targeted specifically against the Organization. However, the personal information was exposed to an individual(s) with nefarious intent. The information could be used by this individual to commit identity theft, fraud, and for phishing. In addition, the Organization has no way to determine if the personal information was accessed or not. The youths are, in my view, a vulnerable group. The youths' dates of birth were involved. The Organization also recognized that it is possible to match the contact information of parents on the database with 179 youths. None of these factors in and of themselves would, in my view, indicate a real risk of significant harm to the affected individuals. However, these factors in combination contributed significantly to my decision that there is a real risk of significant harm to the affected individuals involved in this incident.

V. Decision

[19] I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

[20] I understand that the Organization notified the adults and event coordinators in accordance with the Regulation in correspondence sent on February 8, 2013. Therefore, I will not require the Organization to notify these affected individuals again.

[21] The Organization is able to link 179 youths with adult parents. The notice previously provided to the adult parents of these youths was in accordance with the Regulation. Therefore, I will not require the Organization to notify these youths again.

[22] With respect to the balance of the youths that cannot be linked to adult parents, in accordance with my authority under section 19.1(2) of the Regulation and the ability to provide notice to individuals under the age of 18 pursuant to section 61, I recognize the other steps taken by the Organization to indirectly notify these youths was in accordance with the Regulation. Therefore, I will not require the Organization to notify these youths again.

Jill Clayton
Information and Privacy Commissioner